SENATE COMMITTEE ON PUBLIC SAFETY

Senator Steven Bradford, Chair
2021 - 2022 Regular

Bill No:	SB 1038	**Hearing Date:**	March 15, 2022
Author:	Bradford		
Version:	February 15, 2022		
Urgency:	No	**Fiscal:**	No
Consultant:	AB		

Subject: ***Law enforcement: facial recognition and other biometric surveillance***

HISTORY

Source: ACLU California Action

Prior Legislation: AB 2261 (Chau, 2020), held in the Assembly Appropriations Committee
SB 1186 (Hill, 2018), held in the Assembly Appropriations Committee
SB 21 (Hill. 2017), held in the Assembly Appropriations Committee
AB 1940 (Cooper, 2016), failed passage in Senate Public Safety
AB 69 (Rodriguez) Ch. 461, Stats. of 2015

Support: Asian Americans Advancing Justice – California; Asian Law Alliance; Asian Prisoner Support Committee; California Nurse Association; Black Alliance for Just Immigration; California Coalition for Women Prisoners; California Public Defenders Association; California Attorneys for Criminal Justice; Californians United for A Responsible Budget; Central American Resource Center; CHISPA; Communities United for Restorative Youth Justice; Courage California; Data for Black Lives; Electronic Frontier Foundation; Ella Baker Center for Human Rights; Human Impact Partners; ICE Out of Marin; Immigrant Legal Resource Center; Indivisible SF; Indivisible 49; Initiate Justice; Media Alliance; National Association of Criminal Defense Lawyers; National Center for Lesbian Rights; PICO California; San Francisco Public Defender; Secure Justice; Sonoma County Democratic Party; Stop the Musick Coalition; Young Women's Freedom Center

Opposition: California State Sheriffs' Association; Peace Officers Research Association of California (PORAC)

PURPOSE

The purpose of this bill is to delete the January 1, 2023 sunset date on provisions of law that prohibit a law enforcement officer from installing, activating or using a biometric surveillance system in connection with a body-worn camera or data collected by a body-worn camera. This bill also deletes the sunset on the provision allowing a person to bring an action for equitable or declaratory relief against an agency or officer that violates this prohibition.

Existing law declares that all people are by nature free and independent and have inalienable right, among which are enjoying and defending life and liberty, acquiring, possessing and

protecting property, and pursuing and obtaining, safety, happiness and privacy. (Cal. Const., Art. 1, Sec. 1)

Existing law declares that it is the intent of the Legislature to establish policies and procedures to address issues related to the downloading and storage data recorded by a body-worn camera worn by a peace officer; these policies and procedures shall be based on best practices. (Pen. Code, § 832.18, subd. (a).)

Existing law encourages agencies to consider best practices in establishing when data should be downloaded to ensure the data is entered into the system in a timely manner, the cameras are properly maintained and ready for the next use, and for purposes of tagging and categorizing the data. (Pen. Code, § 832.18, subd. (b).)

Existing law encourages agencies to consider best practices in establishing specific measures to prevent data tampering, deleting, and copying, including prohibiting the unauthorized use, duplication or distribution of body-worn camera data. (Pen. Code, § 832.18, subd. (b)(3).)

Existing law encourages agencies to consider best practices in establishing the length of time that recorded data is to be stored, and states that non-evidentiary data including video and audio recorded by a body-worn camera should be retained for a minimum of 60 days, after which it may be erased, destroyed, or recycled. This provision provides that an agency may keep data for more than 60 days to have it available in case of a civilian complaint and to preserve transparency. (Pen. Code, § 832.18, subd. (b)(5)(A).)

Existing law states that evidentiary data including video and audio recorded by a body-worn camera should be retained for a minimum of two years under any of the following circumstances:

1) The recording is of an incident involving the use of force by a peace officer or an officer-involved shooting;
2) The recording is of an incident that leads to the detention or arrest of an individual; or,
3) The recording is relevant to a formal or informal complaint against a law enforcement officer or a law enforcement agency. (Pen. Code, § 832.18, subd. (b)(5)(B).)

Existing law states that the recording should be retained for additional time as required by law for other evidence that may be relevant to a criminal prosecution. (Pen. Code, § 832.18, subd. (b)(5)(C).)

Existing law instructs law enforcement agencies to work with legal counsel to determine a retention schedule to ensure that storage policies and practices comply with all relevant laws and adequately preserve evidentiary chains of custody. (Pen. Code, § 832.18, subd. (b)(5)(D).)

Existing law encourages agencies to adopt a policy that records or logs of access and deletion of data from body-worn cameras should be retained permanently. (Pen. Code, § 832.18, subd. (b)(5)(E).)

Existing law encourages agencies to include in a policy information about where the body-worn camera data will be stored, including, for example, an in-house server that is managed internally, or an online cloud database that is managed by a third-party vendor. (Pen. Code, § 832.18, subd. (b)(6).)

Existing law instructs a law enforcement agency using a third-party vendor to manage the data storage system, to consider the following factors to protect the security and integrity of the data:

1) Using an experienced and reputable third-party vendor;
2) Entering into contracts that govern the vendor relationship and protect the agency's data;
3) Using a system that has a built-in audit trail to prevent data tampering and unauthorized access;
4) Using a system that has a reliable method for automatically backing up data for storage;
5) Consulting with internal legal counsel to ensure the method of data storage meets legal requirements for chain-of-custody concerns; and
6) Using a system that includes technical assistance capabilities. (Pen. Code, § 832.18, subd. (b)(7).)

Existing law encourages agencies to include in a policy a requirement that all recorded data from body-worn cameras are property of their respective law enforcement agency and shall not be accessed or released for any unauthorized purpose. Encourages a policy that explicitly prohibits agency personnel from accessing recorded data for personal use and from uploading recorded data onto public and social media Internet websites, and include sanctions for violations of this prohibition. (Pen. Code, § 832.18, subd. (b)(8).)

Existing law defines several terms related to the prohibition contained in Pen. Code §832.19(b). (Pen. Code, §832.19, subd. (a)(1)-(9).)

Existing law prohibits a law enforcement agency or officer from installing, activating or using any biometric surveillance system in connection with an officer's body-worn camera or data collected by an officer's body-worn camera. (Pen. Code, §832.19, subd. (b).)

Existing law provides that a person may bring an action for equitable or declaratory relief against a law enforcement agency or officer that violates the prohibition in Penal Code §832.19(b). (Pen. Code, §832.19, subd. (c).)

Existing law provides that this prohibition does not preclude a law enforcement agency or officer from using a mobile fingerprint scanning device during a lawful detention to identify a person who does not have proof of identification, so long as the use of such device does not generate or result in the retention of any biometric data or surveillance information. (Pen. Code, §832.19, subd. (d).)

Existing law provides that the prohibition contained in Penal Code §832.19 is effective only until January 1, 2023, and as of that date is repealed. (Pen. Code, §832.19, subd. (e).)

This bill deletes the January 1, 2023 sunset on the provisions of law that prohibit the use of biometric surveillance systems in connection with body-worn cameras used by law enforcement and provide a cause of action for relief against agencies and officers that violate this prohibition.

This bill makes the following findings and declarations:

- Californians value privacy as an essential element of their individual freedom and are guaranteed a right to privacy in Section 1 of Article I of the California Constitution.

- Existing law, Section 832.19 of the Penal Code, has effectively protected privacy, safeguarded the rights of people exercising First Amendment rights, and prevented the misidentification of Californians and the creation of vulnerable biometric databases since January 1, 2020.

- Section 832.19 of the Penal Code has prevented the waste of critical public resources on ineffective mobile facial recognition programs, including a City of San Diego area facial recognition program that failed to produce a single arrest or prosecution in a seven-year period.

- Facial recognition and other biometric surveillance technology pose unique and significant threats to the civil rights and civil liberties of residents and visitors and would disproportionately pose a threat to marginalized Californians, including people of color and those living in highly policed communities. The use of facial recognition would also diminish effective policing and public safety by discouraging people in these communities, including victims of crime and undocumented persons, from seeking police assistance or from assisting the police.

- The use of facial recognition and other biometric surveillance is the functional equivalent of requiring every person to show a personal photo identification card at all times in violation of recognized constitutional rights. This technology also allows people to be tracked without consent. It would also generate massive databases about law-abiding Californians and may chill the exercise of free speech in public places.

- Facial recognition and other biometric surveillance technology have been repeatedly demonstrated to misidentify women, young people, and people of color and to create an elevated risk of harmful "false positive" identifications. After the Legislature adopted Section 832.19 of the Penal Code, the federal government's gold standard test found that Asian and Black people continue to be 100 times more likely to be misidentified by facial recognition algorithms than white men.

- Prominent technology companies like Microsoft, Amazon, and IBM are declining to sell facial recognition systems to law enforcement. Since the enactment of Section 832.19 of the Penal Code, the prominent body camera maker Axon has also rejected the use of facial recognition for body cameras, citing the potential inaccuracy and abuse.

- Body cameras are fundamentally incompatible with biometric surveillance. This is due to a number of factors, including officers being in near-constant motion, resulting in blurry and low-quality images that will lead to more false matches, as well as the wide-angle images captured body cameras, which result in warped faces that facilitate additional false matches.

- Facial and other biometric surveillance would corrupt the core purpose of officer-worn body-worn cameras by transforming those devices from transparency and accountability tools into roving surveillance systems.

COMMENTS

1. Need for This Bill

According to the author:

> Officer-worn body cameras are fundamentally incompatible with biometric surveillance, in part because officers are in near-constant motion and because the wide angle of the images causes blurred and low-quality images that risks false matches and wrongful arrest. According to research by the National Institute of Standards and Technology (NIST), Asian and Black people were up to 100 times more likely to be misidentified by facial recognition than white men.
>
> Against this background, prominent technology companies like Microsoft, Amazon, and IBM have declined to sell facial recognition systems to law enforcement. Axon, the most prominent body camera maker has also specifically rejected the use of facial recognition for body-worn cameras, citing the potential inaccuracy and serious ethical concerns.
>
> In 2019, the Legislature passed AB 1215 to temporarily prohibit law enforcement in California from adding facial recognition and other biometric surveillance technology to officer-worn body cameras for use against the public. This protection is set to expire on January 1, 2023.

2. Facial Recognition Technology

Facial recognition technology is capable of identifying an individual by comparing a digital image of the person's face to a database of known faces, typically by measuring distinct facial features and characteristics. Early versions of the technology were pioneered in the 1960s and 1970s, but true facial recognition technology as we understand it today did not come about until the early 1990s. In 1993, the United States military developed the Facial Recognition Technology (FERET) program, which aimed to create a database of faces and recognition algorithms to assist in intelligence gathering, security and law enforcement.[1] Since that time, advances in computer technology and machine learning have led to faster and more accurate recognition software, including real-time face detection in video footage and emotional recognition.

Today, facial recognition technology is used in a variety of applications. It is often a prominent feature in social media platforms, such as Facebook, Snapchat and TikTok. For instance, DeepFace, a "deep learning" facial recognition system created by Facebook, helps the platform identify photos of users so they can review or share the content.[2] Snapchat employs similar technology to allow users to share content augmented by "filters," which can add features or alter an image of the user's face. Facial recognition technology has also seen increasing use as a

---

[1] "Facial Recognition Technology (FERET)." The National Institute of Standards and Technology, United States Department of Commerce. https://www.nist.gov/programs-projects/face-recognition-technology-feret

[2] Facebook has recently indicated that it would reduce its use of this technology, but its parent company, Meta, may continue to use it in other applications. See "Facebook is backing away from facial recognition. Meta isn't." 3 November 2021. https://www.vox.com/recode/22761598/facebook-facial-recognition-meta

method of ID verification, such as with Apple's Face ID and Google's Android "Ice Cream Sandwich" systems.

As facial recognition technology has become more widespread, so have concerns about its shortcomings and potential for misuse. Many critics highlight that the use of facial recognition systems result in serious privacy violations, and that mechanisms to protect against the unwanted sale or dissemination of personal biometric data are insufficient.[3] Others suggest that the technology is still too inaccurate and unreliable to be used in such a broad array of applications. For instance, studies suggest that while facial recognition systems have had increasing success identifying cis-gendered individuals, these systems get it wrong more than one-third of the time if the face belongs to a transgender person.[4] However, even among cis-gendered individuals, research shows that facial recognition systems can be significantly less accurate when identifying women than when identifying men.[5] Additionally, a growing body of research demonstrates that facial recognition systems are significantly less accurate in identifying individuals with dark complexions, particularly women.[6]

3. Law Enforcement Uses of Facial Recognition Systems

Despite growing concerns, law enforcement agencies at the federal, state and local level continue to use facial recognition programs. A recent Government Accountability Office report revealed that 20 federal agencies employ such programs, 10 of which intend to expand them over the coming years.[7] Another recent study found that one in four law enforcement agencies across the country can access some form face recognition, and that half of American adults – more than 117 million people – are in a law enforcement face recognition network.[8] Very few of these agencies have a formal facial recognition policy, but one such agency, the New York Police Department, defines the scope of its policy as follows: "Facial recognition technology enhances the ability to investigate criminal activity and increases public safety. The facial recognition process does not by itself establish probable cause to arrest or obtain a search warrant, but it may generate investigative leads through a combination of automated biometric comparisons and human analysis."[9] Proponents of facial recognition technology see it as a useful tool in helping identify criminals. It was reportedly utilized to identify the man charged in the deadly shooting at The Capital Gazette's newsroom in Annapolis, Maryland in 2018.[10]

---

[3] Schwartz, Adam. "Resisting the Menace of Face Recognition." *Electronic Frontier Foundation*. 26 October 2021. https://www.eff.org/deeplinks/2021/10/resisting-menace-face-recognition

[4] "Facial Recognition Software Has a Gender Problem." *National Science Foundation*. 1 November 2019. https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=299486

[5] Buolamwini, Joy, et al. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." PMLR 81:77-91, 2018. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

[6] Najibi, Alex. "Racial Discrimination in Face Recognition Technology." *Harvard University Graduate School of Arts and Sciences Blog.* 24 October 2020. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

[7] "Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks." *United States Government Accountability Office*. 3 June 2021. https://www.gao.gov/products/gao-21-518

[8] Garvie, Clare, et al. "The Perpetual Line-Up: Unregulated Police Face Recognition in America." *The Georgetown Law Center on Privacy and Technology*. 18 October 2016. https://www.perpetuallineup.org/

[9] "Facial Recognition Technology Patrol Guide." *City of New York Police Department.* Issued 12 March 2020. https://www1.nyc.gov/assets/nypd/downloads/pdf/nypd-facial-recognition-patrol-guide.pdf

[10] Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says*, New York Times, July 26, 2018, Available at: https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html?login=facebook.

The inaccuracy, biases and potential privacy intrusions inherent in many facial recognition systems used by law enforcement have led to criticism from civil rights advocates, especially in California. In March 2020, the ACLU, on behalf of a group of California residents, filed a class action lawsuit against Clearview AI, claiming that the company illegally collected biometric data from social media and other websites, and applied facial recognition software to the databases for sale to law enforcement and other companies.[11] An investigation by Buzzfeed in 2021 found that 140 state and local law enforcement agencies in California had used or tried Clearview AI's system.[12] The controversy surrounding law enforcement use of facial recognition has led many California cities to ban the technology, including San Francisco, Oakland, Berkeley, Santa Cruz and Alameda.

In September 2021, the Los Angeles Times reported that the Los Angeles Police Department had used facial recognition software nearly 30,000 times since 2009, despite years of "vague and contradictory information" from the department "about how and whether it uses the technology." According to the Times, "The LAPD has consistently denied having records related to facial recognition, and at times denied using the technology at all." Responding to the report, the LAPD claimed that the denials were just mistakes, and that it was no secret that the department used such technology. Although the department could not determine how many leads from the system developed into arrests, it asserted that "the technology helped identify suspects in gang crimes where witnesses were too fearful to come forward and in crimes where no witnesses existed."[13]

4. AB 1215 (Ting, 2019)

In 2019, the Legislature passed Assembly Bill 1215 (Ting, Ch. 579, Stats. of 2019), which banned the use of facial recognition technology and other biometric surveillance systems in connection with cameras worn or carried by law enforcement, including body-worn cameras (BWC), for the purpose of identifying individuals using biometric data. This ban covers both the direct use of biometric surveillance by a law enforcement officer or agency, as well as a request or agreement by an officer or agency that another officer or agency, or a third party, use a biometric surveillance system on behalf of the requesting party. The ban also includes narrow exceptions for processes that redact a recording prior to disclosure in order to protect the privacy of a subject, and the use of a mobile fingerprint-scanning device to identify someone without proof of identification during a lawful detention, as long as neither of these functions result in the retention of biometric data or surveillance information. AB 1215 included a sunset date of January 1, 2023.

This bill asks the Legislature to consider whether the ban on biometric surveillance and facial recognition systems in connection with cameras worn or carried by officers should remain in effect indefinitely. At its core, this question involves balancing the purported investigatory benefits of facial recognition technology against its demonstrated privacy risks, technical flaws and racial and gender biases. Committee staff has not identified or received evidence

---

[11] "Clearview AI class-action may further test CCPA's private right of action." *JD Supra.* 12 March, 2020. https://www.jdsupra.com/legalnews/clearview-ai-class-action-may-further-14597/

[12] "Your Local Police Department Might Have Used This Facial Recognition Tool To Surveil You. Find Out Here." *Buzzfeed News.* 6 April 2021. https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table

[13] "Despite past denials, LAPD has used facial recognition software 30,000 times in last decade, records show." *Los Angeles Times.* 21 September 2020. https://www.latimes.com/california/story/2020-09-21/lapd-controversial-facial-recognition-software

demonstrating that the ban on facial recognition technology used in connection with BWC has significantly hampered law enforcement efforts in the two years since it became operative.

5. Argument in Support

Writing in support of the measure, advocacy organization Secure Justice argues:

> Face recognition-enabled police body cameras permit pervasive and ongoing surveillance of the public, registering and reporting who we are and where we go. Allowing face and biometric systems to be added to police body cameras would threaten the civil rights and civil liberties of all residents and visitors and pose a disproportionate threat to marginalized Californians, including people of color and those living in highly policed communities.
>
> Facial recognition has also been repeatedly demonstrated to misidentify women, young people and people of color.2 Members of the California legislature and the California Congressional delegation have experienced this disproportionate error rate firsthand in tests comparing them against mug-shot databases.3 Multiple Black men have been wrongfully arrested in other states due to false matches. If a police body camera with facial recognition misidentified a person, that error could misinform an officer's decision about how to approach a person or even use of deadly force. SB 1038 reinforces the California law that helps prevent similar life-changing mistakes.
>
> Finally, if California was to allow the use of body camera face surveillance, it would lead to the creation of face-recognition databases that are susceptible to data breaches and are likely to be exploited by agencies like U.S. Immigration and Customs Enforcement (ICE) - an agency that has already demanded other states run face searches on its behalf. California has refused to create a surveillance network that invites anti-immigrant exploitation by the Federal government, and it should continue to stand for the rights of immigrants.

6. Argument in Opposition

According to the Peace Officers Research Association of California (PORAC):

> PORAC uses facial recognition to identify criminals in situations where we know that a possible threat could occur in a crowd, or it's used on captured video to search for a dangerous criminal. The number of dangerous crimes thwarted by utilizing this technology completely justifies its continued use. Lastly, as technology evolves, it is essential for law enforcement to grow with it. Technology helps us do our jobs more efficiently and ultimately improves public safety.

-- END –